إضاءات

نشرة توعوية يصدرها
معهد الدراسات المصرفية

مستقبل المخاطر في العصر الرقمي

The Future Of Risk In The Digital Era

السلسلة 15 | العدد 2

دولة الكويت | نوفمبر - 2022

1. مقدمة

يشهد العالم تقدماً متسارعاً في عصر التكنولوجيا الرقمية بشكل غير مسبوق، حيث وصلت التكنولوجيا الرقمية إلى حوالي 50% من سكان الدول النامية في أقل من عقدين، وأحدثت تحولاً ملحوظاً في أغلب المجتمعات. وبالتالي يصفها البعض بأنها من أهم عوامل تحقيق المساواة في العصر الحديث، ويصفها آخرون بأنها السبب في إنتاج عديد من المخاطر والتحديات غير المسبوقة، التي أدت إلى حدوث انتهاكات للخصوصية، وإرهاب إلكتروني واختراق للبيانات، لذلك سارعت الدول والمؤسسات إلى إيجاد حلول لتعظيم الاستفادة من التكنولوجيا الرقمية من ناحية، والعمل على تجنب المخاطر المترتبة عليها وتقليلها من ناحية أخرى.

2. الثورة الرقمية وعصر المعلومات

الثورة الرقمية أو ما يطلق عليها (الثورة الصناعية الرابعة)، حيث تتجه أنظار العالم إلى رقمنة كل ما يحيط بالإنسان، وذلك من خلال إنتاج عديد من التقنيات الحديثة، التي ساعدت على خلق فرص جديدة ومتنوعة، كما أنها أحدثت تغيراً في حياة الأفراد وطريقة تعاملهم فيما بينهم وتجاه الأشياء، ومن خلال تسارع التطورات التقنية الحديثة وتطبيقها في عديد من المجالات ورقمنة كثير من الخدمات، برزت تقنيات عدة، منها: إنترنت الأشياء (IoT) والذكاء الاصطناعي (AI) وتقنية سلسلة الكتل (Blockchain)، والحوسبة السحابية (cloud computing) والتعليم الآلي (machine learning) والبيانات الضخمة (Big data) وغيرها، ومكنت تلك التقنيات المؤسسات والدول من استخراج وتحليل كثير من المعلومات والبيانات التي ساعدت الشركات على فهم سلوك الأفراد ورغباتهم، وبالتالي تحسين عملية اتخاذ القرارات على جميع المستويات، كما ساهمت الثورة الرقمية في التخلص من آلاف السجلات الورقية التي كانت تستغرق فترات طويلة من الوقت للبحث عن معلومة، وحلت مكانها آليات تقنية لديها القدرة على الوصول إلى المعلومات والبحث عنها في بضع ثوانٍ، موفرةً بذلك الوقت والجهد والتكلفة.

3. ما هو مفهوم إدارة المخاطر الرقمية؟

كما قدم عصر المعلومات والثورة الرقمية مزايا كثيرة لقطاع الخدمات المالية ومختلف القطاعات الأخرى (كالصحة - التعليم - السياحة - الصناعة - التجارة، وغيرها)، إلا أنه أنتج كذلك عديدًا من المخاطر التي تحتاج إلى إدارة ومعالجة بشكل مستمر، لذلك أصبح مفهوم إدارة المخاطر الرقمية موضعًا لكثير من البحث والتطوير، ولا يختلف كثيراً مفهوم إدارة المخاطر الرقمية عن المفهوم التقليدي لإدارة المخاطر، حيث يركز مفهوم إدارة المخاطر بشكل عام على «تحديد المخاطر وتقييمها وترتيب أولوياتها، ويتبع ذلك استخدام اقتصادي للموارد، من أجل تقليل احتمالية أو تأثير الأحداث السلبية ومراقبتها أو التحكم فيها لتحقيق أقصى قدر ممكن من الفرص»، وذلك كما نص عليها الدليل الإرشادي لإدارة المخاطر، الصادر عن وزارة الاتصالات وتقنية المعلومات السعودية لعام 2021.

وقد عرفت الجمعية المهنية الدولية لحوكمة تكنولوجيا المعلومات آيزاكا (ISACA) إدارة المخاطر الرقمية على أنها «عملية تحديد نقاط الضعف والتهديدات لموارد المعلومات التي تستخدمها أي جهة أو مؤسسة في تحقيق أهدافها، وتحديد الإجراءات المضادة، التي يجب اتخاذها للحد من المخاطر إلى مستوى مقبول، بناءً على قيمة موارد المعلومات للمؤسسة»، وبالتالي يرتكز كلا التعريفين على تحديد التهديدات والمخاطر التي توقع الضرر بالمؤسسة، ومن ثم اتخاذ إجراءات معينة تجاه هذه التهديدات لتقليل مستوى هذه المخاطر، وبلا شك تتنوع أشكال هذه المخاطر والتهديدات بشكل مستمر خاصة في العصر الرقمي الذي يتسم بالنمو المتسارع والمتغير، لذلك نركز في هذه الإضاءة على أنواع المخاطر الرقمية بشكل مختصر في الفقرة التالية.

4. ما أنواع المخاطر الرقمية؟

أولاً: مخاطر رقمنة المعلومات

من المخاطر التي استجدت نتيجة رقمنة المعلومات منها:

- سهولة انتشار المعلومات الضارة أو الأخبار السيئة أو الإشاعات التي توقع ضرراً على المجتمعات أو المؤسسات أو الأفراد، وذلك من خلال الاستغلال الخاطئ للمنصات الرقمية التي تجمع عددًا ضخمًا من المستخدمين.
- اختراق المعلومات من خلال هجمات إلكترونية يصعّب ملاحقة منفذيها، وقد تستهدف أفرادًا أو مؤسسات أو دولًا، وذلك من خلال إرسال فيروسات أو استغلال ثغرات في أنظمة التشغيل الإلكتروني مثل فيروس (ransomware) حيث يقوم بتشفير الملفات ويمنع الوصول إليها، وغالباً ما تطلب الجهات التي تقوم به مقابلًا باهظ التكلفة لإزالة هذا التشفير.
- إحداث تحولات اقتصادية تضر بالأفراد والمؤسسات، مثل عمليات التحول من الهياكل التقليدية إلى هياكل جديدة تناسب التحول الرقمي، وبالتالي يتضرر المستفيدون من الهياكل التقليدية، وقد يصل الأمر إلى فقدان بعض الشركات قدراتها التنافسية المحلية والدولية بسبب الابتكارات الرقمية المتنوعة التي قد تجعل بعض الشركات تتراجع بل قد تختفي نتيجة التطور المستمر، ومثال لذلك شركة (Nokia) التي تكاد تكون اختفت من أسواق الأجهزة الإلكترونية بسبب تسارع الشركات المنافسة لها في استخدام التكنولوجيا الرقمية.
- مخاطر الهندسة الاجتماعية، وهي تتلخص في استغلال الضعف البشري من خلال القيام بالاحتيال في صورة محاكاة مصدر موثوق، حيث يتظاهر المحتال بأنه من فريق مكتب مساعدة تكنولوجيا المعلومات أو من فريق الدعم الفني أو غير ذلك، وقد يتواصل عبر رسائل البريد الإلكتروني أو الرسائل النصية أو المكالمات للحصول على معلومات سرية، مثل بيانات اعتماد الوصول إلى الحسابات المصرفية أو محاولة الوصول إلى شبكات البيانات للمؤسسات، وغير ذلك.

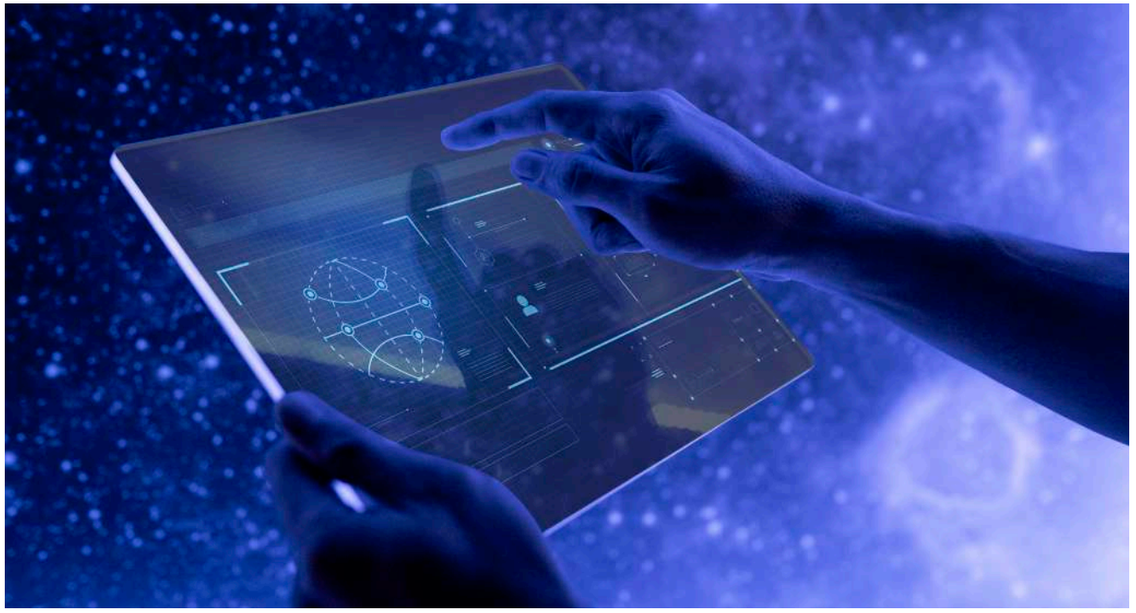
ثانياً: المخاطر الاجتماعية

على الرغم من الازدهار الذي أحدثه العصر الرقمي والمزايا العديدة التي حققها للبشرية، إلا أنه ترك آثارًا سلبية كذلك تضر بعادات المجتمعات وتقاليدها وبنيتها الأساسية، ومن ذلك:

- أصبحت العلاقات الاجتماعية في عديد من المجتمعات، هشة وغير مستقرة في كثير من الأحيان، حيث بات أغلب الأفراد يقضون أكثر أوقاتهم على العالم الافتراضي، وأدى ذلك إلى حالة من العزلة عن العالم الحقيقي، مما تسبب في ظهور كثير من المشكلات التي تضر بالمجتمع وأفراده.
- ويعد الشباب والأطفال الفئة الأكثر تعرضاً للمخاطر الاجتماعية في العصر الرقمي، حيث أصيب كثير من الشباب بحالة من الإدمان للعالم الافتراضي والألعاب، مما تسبب في تعسر في التعامل مع العالم الحقيقي، ونتج عن ذلك عدم رغبة كثير منهم في مواجهة مسؤوليات الحياة وتحدياتها.
- من ضمن المخاطر الاجتماعية للعصر الرقمي تعزيز الثقافة الاستهلاكية، حيث يجد الأفراد في العالم الرقمي ما يمكن أن يحقق لهم الإشباع، حتى ولو لم يحقق ذلك فائدة حقيقية لهم، وبالتالي الاستهلاك المفرط للوقت والموارد، مما قد يخفض إنتاجية الأفراد والمؤسسات، ونفاد الموارد مقابل الزيادة المستمرة للرغبات.

ثالثاً: مخاطر الخصوصية وتبادل المعلومات

- أصبحت جميع الأجهزة الذكية وتطبيقات الهاتف الذكي والبرامج المتقدمة وسائل لجمع البيانات عن الأفراد من حيث سلوكهم الشرائي وأفكارهم ورغباتهم، وبالتالي تعمد الشركات التقنية التي تهتم بسلوك العملاء إلى تخزين هذه البيانات ومعالجتها وتحليلها، وعلى الرغم مما تنص عليه مواثيق هذه الشركات من عدم استخدام البيانات إلا فيما يتعلق بالأمور التسويقية لمساعدة العميل للوصول بسهولة لاحتياجاته، إلا أن الحصول على بيانات العملاء لا تخلو من تعرضها لمخاطر استخدامها لأغراض أخرى.
- أيضاً تناقل البيانات الرقمية بين الأفراد والمؤسسات أو الدول، يجعلها عرضة للهجمات الإلكترونية، وقد لا تستطيع شبكات الحماية في بعض الأحيان توفير الحماية الكاملة أو المطلقة للبيانات، وهو ما يهدد خصوصية الأفراد والمؤسسات والدول لمخاطر تبادل المعلومات.



رابعاً: مخاطر الإرهاب الإلكتروني والقرصنة في العصر الرقمي

عرفت بعض الدراسات الإرهاب الإلكتروني بأنه عبارة عن هجمات أو تهديدات ضد أنظمة الحاسب أو شبكات الانترنت أو البيانات المخزنة بشكل رقمي من أجل التأثير السلبي على الأفراد أو المؤسسات أو حتى الدول، وبالتالي يختلف الاختراق الإلكتروني عن الإرهاب الإلكتروني في أن الأخير يتبع عملية الاختراق أو التهديد أو التخويف أو إلحاق الضرر بالآخرين.

وتتعدد أشكال الإرهاب الإلكتروني والقرصنة بوسائل وطرق مختلفة، منها:

• تدمير البيانات والمواقع الإلكترونية والنظم المعلوماتية

حيث تعتمد غالبية أنظمة المؤسسات على الحاسوب والإنترنت في تسيير أعمالها، فقد تُستخدم هجمات الإرهاب الإلكتروني لتدمير البيانات والمواقع الإلكترونية، لتحقيق أهداف عدائية تؤثر سلباً على المؤسسات والدول، ومن ذلك على سبيل المثال: التحكم في بعض المواقع الخاصة بتقديم الخدمات الطبية والتعليمية والمالية وخطوط الطيران وغير ذلك من الأهداف، وهو ما يعود بضرر بالغ الأثر على اقتصادات الدول واستقرارها.

• تهديد وترويع الآخرين

يتم ذلك من خلال أفراد أو مجموعات يقومون باستخدام التهديد والترويع لتحقيق بعض المنافع المالية والسيطرة من خلال طرق مختلفة، سواء بإرسال رسائل مباشرة بالتهديد والتنكيل أو الأذى في حال الإقدام أو الإحجام عن فعل بعض الأمور، وقد تكون من خلال رسائل نصية أو صور وفيديوهات تُظهر قوة الجهة القائمة بالتهديد، وبالتالي بث الرعب والتخويف للجهة المستهدفة.

- **اختراق المواقع الإلكترونية**

عادة ما يكون الاختراق لتعطيل أنظمة تشغيل لمؤسسات، أو سرقة معلومات سرية، ثم يتم استخدام تلك البيانات في تحقيق بعض الأغراض التي تسعى إليها الجهة المنفذة مقابل هذه المعلومات كطلب أموال طائلة في مقابل إرجاع هذه البيانات، وغيرها من الأغراض غير المشروعة التي تسعى إليها الجهة المنفذة للاختراق.

- **التجسس الإلكتروني**

غالباً ما يتم ذلك لمعرفة معلومات سرية لدى مؤسسات كبرى أو شخصيات مثيرة للجدل، أو يتم أيضاً بين بعض الدول، ويُستخدم عادة أحدث الوسائل والتقنيات المتطورة للقيام بالتجسس الإلكتروني، وهو ما يمثل مخاطر كبيرة للدول والمؤسسات، والأفراد.

خامساً: مخاطر العمليات التجارية (التجارة الإلكترونية)

- في المنصات الرقمية الخاصة بالتجارة الإلكترونية يترك المستخدم العديد من الآثار التي يمكن من خلالها معرفة ميوله وفهم سلوكه، من خلال المواقع التي قام بزيارتها، والمحتوى الذي قام بتنزيله، والبضائع التي قام بشرائها وغير ذلك من المعلومات الدقيقة التفصيلية عن الأمور الخاصة بالأفراد، وبالتالي يتعرض الأفراد لمخاطر استغلال معلوماتهم من خلال تبادلها بين المتاجر الإلكترونية مما ينتج عنه اختراق لخصوصية الأفراد بأشكال مختلفة، مثل التواصل معه بطرق مختلفة دون إذنه، وتفعيل اشتراكه في منصات دون تصريح منه.
- وبسبب تحول الكثير من المتاجر التقليدية إلى متاجر إلكترونية، تقوم المتاجر الإلكترونية بطلب الكثير من البيانات المتعلقة بالعميل بهدف التأكد من هويته وعدم وقوع احتيال أو سرقة، مثل طلب اسم المستخدم وأرقام التواصل معه (الهاتف - مواقع التواصل الاجتماعي - وعنوانه، ومعلومات أخرى حول الجنس والسن والحالة الاجتماعية) وغير ذلك من التفاصيل التي قد تكون ليس لها علاقة بعملية الشراء الحالية للعميل، إلا تجميع قاعدة واسعة من بيانات العملاء، قد تؤدي إلى تعرضه للمخاطر في حالة سوء استخدام هذه البيانات، وتعرضها لمخاطر متنوعة من الغش والخداع والاحتيال عبر التجارة الإلكترونية.
- بالإضافة لذلك، هنالك مخاطر سرقة الأموال من خلال كتابة العميل بيانات بطاقة الدفع الخاصة به من حيث نوع البطاقة ورقمها وتاريخ انتهائها، وغير ذلك مما قد يعرض بطاقات العملاء للاحتيال والسرقة في حالة التعرض لهجمات إلكترونية على منصات التجارة الإلكترونية كونها هدفاً كبيراً لمنفذي الهجمات الإلكترونية.

سادساً: مخاطر البنية التحتية الرقمية

تعتمد البنية التحتية الرقمية بشكل رئيسي على مراكز البيانات وخوادم التشغيل وبرامج الحوسبة السحابية، وشبكات الاتصالات وغيرها مما يساهم في تشغيل وتطوير التكنولوجيا الرقمية، وكما تتعرض الخدمات الرقمية للعديد من المخاطر، كذلك تتعرض البنية التحتية التي تعمل على تغذية الخدمات الرقمية إلى كثير من المخاطر، مما يجعل المؤسسات والدول حريصة على حماية البنية التحتية الرقمية بجوانبها المتعددة من المخاطر المختلفة التي تتعرض لها، ومنها:

- التعرض للتهديدات المستمرة المتطورة (Advanced persistent threat (APT)، حيث تقوم مجموعات ذات خبرات عالية في مجال الاختراق بمحاولة اختراق البنية التحتية الرقمية والاستحواذ على كل ما فيها من بيانات ومعلومات أو تدميرها بشكل كامل.

- التعرض لمخاطر هجمات تعطيل توزيع الخدمات (Distributed denial-of-service (DDoS) attacks)، حيث يتم الضغط على الشبكة أو خوادم التشغيل الرئيسية من خلال عمل حركة مرور وهمية مزدحمة لزيادة الضغط على خوادم التشغيل، مما يؤدي إلى تعطيل شبكات الاتصالات والبنية التحتية، وهو ما يجعل المستخدمين غير قادرين على الاتصال أو الوصول إلى الخدمات أو التطبيقات المرغوبة. وبالتالي الوقوع في خسائر مادية كبيرة على المؤسسات وفي بعض الأحيان أنظمة الدول، بسبب استغراق وقت طويل لمعالجة هذه المشكلات.

- في تقرير أعدته IJGlobal لعام 2021، من خلال استبيان قامت به، تبين أن حوالي ثلثي المخاطر الخاصة بالبنية التحتية الرقمية جاءت من خلال الهجمات السيبرانية، ويأتي ذلك نتيجة سهولة انتقال البيانات عبر الإنترنت، والذي ساهم في تسهيل عملية اختراقها، وقد ذكر التقرير أن الولايات المتحدة الأمريكية ستقوم بإنفاق حوالي 22 مليار دولار عام 2022 فقط على الأمن السيبراني، وأن البنوك الكبيرة مثل JP Morgan Chase و Bank of America تصل نفقاتها إلى حوالي 500 مليون دولار سنويًا لحماية العمليات الرقمية، وأن إجمالي الشركات والمؤسسات الخاصة حول العالم وصل إنفاقها تقريباً إلى حوالي تريليون دولار في نهاية 2021، حيث شهد العالم هجمات إلكترونية متعددة في الآونة الأخيرة مثل الهجمة الإلكترونية في ديسمبر 2020 التي شنتها وكالة الاستخبارات الأجنبية الروسية SVR على نظام إدارة شبكة Solarwinds الذي يستخدمه 300,000 عميل في جميع أنحاء العالم.

5. كيفية إدارة المخاطر، ودور الأمن السيبراني

بسبب تزايد المخاطر وتنوعها بشكل ملحوظ كما سبق ذكرها، استدعى ذلك إيجاد وسائل وآليات لإدارة المخاطر بهدف تجنب وتخفيف الأضرار الناتجة عن تلك المخاطر، وتحقيق الاستفادة القصوى من التكنولوجيا الرقمية وعصر المعلومات، وتمر عملية إدارة المخاطر بعدة مراحل كالآتي:

المرحلة الأولى: تحديد دائرة المخاطر وتحليلها

يتعرض الأفراد أو المؤسسات لأشكال متنوعة من المخاطر سواء الاختراق أو التجسس أو تدمير البيانات أو غيرها، لذلك تركز الخطوة الأولى على تحديد الأسباب الرئيسية أو المحتملة لوقوع نوع الخطر، ومدى تأثيره، والأضرار المترتبة على هذا الخطر، وبالتالي تستطيع المؤسسة تحديد طريقة التعامل مع هذا النوع من المخاطر.

المرحلة الثانية: قياس وتقييم مستوى الخطر

في هذه المرحلة يتم حساب حجم المخاطر المحتملة، ونسبة وقوعها، وحجم التكلفة المتوقعة لمعالجتها، وفي حالة وجود عدة مخاطر، يتم التعامل معها حسب درجة أولويتها، وبالتالي يتم التعامل مع الأعلى خطراً ثم الأقل فالأقل. ويتم احتساب المخاطر عن طريق البيانات الكمية وهي الطريقة الأكثر دقة، حيث يتم الوقوف على حجم الخطر الحقيقي من خلال البيانات المتوفرة، وفي حالة عدم توافر البيانات الكمية أو عدم صلاحيتها بسبب حدوث تغيرات جوهرية في البيانات المتاحة، فيتم قياس المخاطر بالاعتماد على الطرق الوصفية، ومنها مصفوفة قياس المخاطر، ويتم ذلك من خلال الاعتماد على متغيرين رئيسيين، وهما حجم الخسارة ومعدل تكرار الخسارة، كما هو مبين في الجدول الآتي:

مصفوفة قياس المخاطر

حجم الخسارة						
	عالي جداً	4	5	6	7	8
	عالي	3	4	5	6	7
	متوسط	2	3	4	5	6
	منخفض	1	2	3	4	5
	منخفض جداً	0	1	2	3	4
		منخفض جداً	منخفض	متوسط	عالي	عالي جداً
		معدل تكرار الخسارة				

المصدر: بتصرف من الدليل الإرشادي لإدارة المخاطر في قطاع الاتصالات وتقنية المعلومات – وزارة الاتصالات وتقنية المعلومات – السعودية، 2021

المرحلة الثالثة: اتخاذ القرار المناسب وتقييمه:

بعد مراجعة كافة البيانات وأسباب المخاطر الحالية والمحتملة، فإن المؤسسة تقوم باتخاذ القرار المناسب لتجنب وقوع المخاطر أو العمل على تقليلها، وقد تشمل القرارات التي تتخذها المؤسسة تغيرًا في الرؤية أو الرسالة أو الأهداف أو خطة العمل والميزانية وغير ذلك بما يتناسب مع وضع تقييم المخاطر في المؤسسة.

وفيما يتعلق بدور الأمن السيبراني، فقد توصل التطور التقني لبناء منهجية واضحة للتصدي للهجمات الإلكترونية وكيفية التعامل مع الهجمات السيبرانية غير المكتملة والناجحة والعمل على اكتشاف التهديدات الإلكترونية وحماية الأنظمة، وقد حرصت كثير من الدول على تعزيز مكانة ودور الأمن السيبراني للتعامل مع المخاطر السيبرانية (Cyber Resilience)، وعلى سبيل المثال فقد قامت دولة

الكويت من خلال بنك الكويت المركزي بإصدار الإطار الإستراتيجي للأمن السيبراني من أجل تحقيق أربعة أهداف رئيسية تشمل:

- تعزيز إجراءات الحماية وأمن المعلومات للقطاع المصرفي.
- تنسيق كافة الجهود لترسيخ مستويات الحماية من المخاطر.
- تشكيل إطار متكامل للتعامل مع المخاطر السيبرانية.
- تحقيق الاستفادة من مزايا التكنولوجيا في القطاع المصرفي والمالي.

6. مبادرات دولة الكويت للتوعية المصرفية والمالية

ضمن مبادرات دولة الكويت للتوعية المصرفية والمالية أعلن بنك الكويت المركزي بالاشتراك مع اتحاد مصارف الكويت، عن إطلاق حملة «لنكن على دراية» التي تهدف إلى نشر الثقافة المالية وزيادة الوعي لدى الجمهور، من أجل تقليل محاولات الاحتيال والخداع الإلكتروني، حيث تعتبر عمليات الاحتيال الإلكتروني من أكثر مخاطر العصر الرقمي تجاه الأفراد، والتي تحدث في شكل سرقات للأموال من حسابات العملاء البنكية، عن طريق إفصاح العملاء عن بياناتهم الشخصية البنكية، أو عبر الضغط على روابط مجهولة المصدر، لذلك ركزت الحملة من خلال الرسائل التوعوية المتنوعة على أن البنك لن يطلب معلومات شخصية عن طريق البريد الإلكتروني أو الرسائل النصية أو المكالمات الهاتفية.

كما أوصت الحملة بضرورة التعامل بحذر مع الروابط الإلكترونية وعدم حفظ أي معلومات سرية مثل: أرقام بطاقة السحب الآلي، أو بطاقة الائتمان، أو رقم التعريف الشخصي على الهاتف النقال. وكذلك عدم كتابة الرقم السري على البطاقة أو مشاركته مع أي جهة. كما أوصت بضرورة تسجيل الخروج من التطبيق أو الموقع الإلكتروني للبنك فور انتهاء أي معاملة، وتطرقت الحملة أيضاً إلى التحذير من المخاطر المتعلقة بالتعامل أو الاستثمار في الأصول الافتراضية (العملات الرقمية)، حيث أنها قد تسبب للمتعامل بها خسائر فادحة، كما أنها غير مرخصة وغير خاضعة لأي جهة رقابية، وبالتالي قد يؤدي التعامل بها إلى حدوث عمليات احتيال ينتج عنها خسائر كبيرة.

ومن المبادرات أيضاً التي أطلقها بنك الكويت المركزي مبادرة «كفاءة»، بالتعاون مع معهد الدراسات المصرفية، وذلك لتأهيل الشباب الكويتي للعمل في المجالات المصرفية والمالية، والتي أطلق من خلالها برنامج «قادة الأمن السيبراني»، الذي يهدف إلى إعداد متخصصين في أمن المعلومات بما يتناسب مع متطلبات القطاع المصرفي المالي، وأيضاً برنامج «قادة إدارة المخاطر الذي يهدف إلى تطوير وتأهيل الكفاءات الوطنية العاملة في قطاع إدارة المخاطر، سواء في القطاع المصرفي أو في القطاعات المماثلة، لمواكبة التطورات العالمية والمحلية في الصناعة المالية في مجال إدارة المخاطر.

يضاف إلى ذلك حصول بنك الكويت المركزي على تجديد لشهادة المعيار العالمي ISO/IEC 27001:2013 الخاص بإدارة أمن المعلومات، ويُعد هذا المعيار أحد أبرز المعايير الدولية التي تنظم آلية بناء وتطبيق السياسات والإجراءات الخاصة بأمن المعلومات في المؤسسات وتحقيق أعلى درجات الكفاءة في تنفيذها، خاصة في ضوء التحديات التي يفرضها التطور التقني المستمر في القطاع المصرفي وقطاع الخدمات المالية، حيث تساهم هذه الشهادة في تطوير ومراقبة نظم حماية أمن المعلومات عن طريق دراسة الأنظمة وتقييم أهميتها، وكذلك تقييم المخاطر المتوقعة وتقديم الحلول التقنية أو التشغيلية التي بدورها تساهم في إدارة المخاطر بفعالية وكفاءة.

7. الخاتمة

استطاعت بالفعل ثورة التكنولوجيا الرقمية وعصر المعلومات تقديم كثير من المنافع للبشرية في جوانب الحياة كافة (الاقتصادية والتعليمية والصحية والاجتماعية والسياسية والعسكرية) من حيث جودة وسرعة الوصول للمعلومات الذي نتج عنه جودة أعلى في اتخاذ القرارات وقدرة أكبر على التحليل والتقييم والتطوير وكفاءة أعلى في إنجاز الأعمال. ولكن من جانب آخر أنتجت الثورة الرقمية كثيرًا من المخاطر بأشكال متعددة، مثل مخاطر الخصوصية وتبادل المعلومات ومخاطر الإرهاب الإلكتروني والاختراق وتدمير البيانات والتجسس وغيرها، مما ترتب عليه كثير من السلبيات والتحديات التي تؤثر على حياة الأفراد والمؤسسات والدول، وهو ما يستدعي إدارة تلك المخاطر والتحديات لتجنبها أو تقليلها من أجل تحقيق الاستفادة القصوى من مزايا ثورة التكنولوجيا والعصر الرقمي.

المراجـــع

بنك الكويت المركزي بالتعاون مع اتحاد مصارف الكويت، حملة لنكن على دراية،
https://www.dirayakw.com/en

بنك الكويت المركزي، 2021، حصول البنك الكويتي المركزي على شهادة المعيار العالمي لأمن المعلومات،
https://www.cbk.gov.kw/ar/cbk-news/announcements-and-press-releases
/press-releases/2021/07/202107050800-cbk-maintains-information-security-iso-certification

بنك الكويت المركزي، 2017، بنك الكويت المركزي يعلن عن إطلاق برنامج قادة الأمن السيبراني،
https://www.cbk.gov.kw/ar/cbk-news/announcements-and-press-releases/press-releases/2017/11/
201711140841-press-release-cbk-announces-the-launch-of-the-cyber-security-leaders-program-cslp

بنك الكويت المركزي، 2020، الانتهاء من بناء الإطار الاستراتيجي للأمن السيبراني للقطاع المصرفي في دولة الكويت،
https://www.cbk.gov.kw/ar/cbk-news/announcements-and-press-releases/press-releases/
2020/02/202002181127-cbk-introduces-cyber-security-framework-for-the-kuwaiti-banking-sector

بنك الكويت المركزي، 2018، إطلاق الدورة الثانية من برنامج قادة الأمن السيبراني،
https://www.cbk.gov.kw/ar/cbk-news/announcements-and-press-releases/press-releases/2018/12/
201812150841-press-release-cbk-governor-announces-launch-of-second-round-of-cyber-security

وزارة الاتصالات وتقنية المعلومات السعودية، 2021، دليل إرشادي "إدارة المخاطر في قطاع الاتصالات وتقنية المعلومات" ص: 26.

خليل، تأثير الثورة الرقمية على مجال الوظيفة، Journal of Urban Research، م (12)، 2014. ص 2.

النحاس، إدارة مخاطر التحول الرقمي، المجلة العلمية للدراسات والبحوث المالية والإدارية، م (13) ع (3). 2022. ص 1503.

الموسوي، الخصوصية المعلوماتية وأهميتها، ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية، 2013.

الدهشان، الإرهاب في العصر الرقمي (الإرهاب الإلكتروني): صوره، مخاطره، آليات مواجهته،
International Journal of Research in Educational Science، م (1) ع (3). 2018. ص 94 - 104.

العرادة، دور إدارة مخاطر التحول الرقمي في تحسين جودة التقارير المالية بالبيئة الكويتية: دراسة ميدانية،
المجلة العلمية للدراسات والبحوث المالية والإدارية. م (8)، ع (2). 2020. ص 5.

IJGlobal, Special Report 2021, The Global Digital Infrastructure Survey,
file:///C:/Users/m.biuomy/Downloads/IJGlobal%20DI%20Survey%202021_e6d066.pdf

معهد الدراسات المصرفية

INSTITUTE OF BANKING STUDIES

ص.ب 1080 الصفاة – 13011 الكويت

P.O.Box 1080 Safat 13011 Kuwait | Tel.: +965 22901100 | Fax: +965 22466430

ibs_kuwait | IBSKuwait | www.kibs.edu.kw | cs@kibs.edu.kw